REMARKS

In response to the non-final action of November 16, 2005, Applicants request that all claims be allowed in view of the amendment to the claims and the following remarks.

Claims 1-45 are pending with claims 1, 21, and 34 being independent. Claims 1, 4, 6, 8, 19, 21, 24, 26, 28, 33, 34, 37, 39, and 40 have been amended. Support for these amendments may be found in the application at, for example, page 19, lines 16-19 and FIG. 10d.

Rejections under the Doctrine of Obviousness-Type Double Patenting

Claims 1-9, 12-14, 21-33, and 34-45 were provisionally rejected under the doctrine of obviousness-type double patenting as being unpatentable over claims 1-9, 10-12, 43-53, 55, 56, and 61-72 of co-pending Application No. 09/810,421. Applicants will address the provisional obviousness-type double patenting rejection upon indication that the claims are otherwise allowable.

Rejections under 35 U.S.C. 103(a)

Claims 1, 21, and 34 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,693,878 ("Daruwalla"). Alternatively, claims 1, 21, and 34 were rejected under 35 U.S.C. 103(a) as being unpatentable over Network Telesystems, NTS Tunnel Builder User's Guide ("NTS") in view of Newswire Association Inc., "Ramp Networks Announces Comprehensive Virtual Network Solution; Targets Corporate Branch Offices" ("Ramp"). Alternatively, claims 1, 21, and 34 along with their dependent claims were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent Number 6,671,739 ("Reed") in view of U.S. Patent Number 6,167,120 ("Kikinis") and in further view of Daruwalla.

Applicants have amended claims 1, 21, and 34 to obviate these rejections.

As amended, claim 1 recites a system for connecting multiple home-networked client devices to a host system, wherein the host system assigns independent Internet addresses to the home-networked client devices. The system includes a home gateway device which includes a communication device to communicate with the host system over a single communication tunnel

established between the home gateway device and the host system. The home gateway device includes a network address translation module. The system also includes multiple home-networked client devices connected to the home gateway device via a network and that communicate with the host system through the home gateway device over the single communication tunnel. The host system is located at one end of the single communication tunnel. The host system is configured to establish individual communication sessions with the multiple home-networked client devices over the single communication tunnel and to assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel.

Applicants respectfully request reconsideration and withdrawal of these rejections because the cited references, either alone or in combination, fail to describe or suggest at least "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1 and similarly recited in claims 21 and 34.

Claim 21 recites a method for connecting multiple home-networked client devices to a host system, wherein the host system assigns independent Internet addresses to the home-networked client devices. The method includes, among other features, "using the home gateway device to receive independent Internet addresses from the host system, located at one end of the single communication tunnel, for each of the multiple home-networked client devices over the single communication tunnel." Similarly, claim 34 recites a similar method that includes, among other features, "using a host system, located at one end of a single communication tunnel, to assign independent Internet addresses to each of multiple home-networked client devices over the single communication tunnel."

In subsequent paragraphs, Applicants in turn address each of the alternate rejections under 35 U.S.C. 103(a). First, Applicants address the Daruwalla rejection. Second, Applicants address the NTS in view of Ramp rejection. Lastly, Applicants address the Reed and Kikinis in view Daruwalla rejection.

A. Daruwalla Rejection

Claims 1, 21, and 34 were rejected under 35 U.S.C. 103(a) as being unpatentable over Daruwalla. Applicants respectfully assert that Daruwalla fails to describe or suggest at least "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1 and similarly recited in claims 21 and 34.

Daruwalla relates to "methods and apparatus for facilitating processing and routing of packets in Virtual Private Network." Daruwalla at col. 1, lines 5-10. Referring to FIG. 3, Daruwalla discloses a high frequency cable network that includes several cable modems. Daruwalla at col. 6, lines 35-40. Each of the "cable modems may service one or more devices which sit behind the cable modem." Daruwalla at col. 6, lines 40-42. The cable modems communicate with a Head End of the high frequency cable network to interact with nodes outside the cable network. Daruwalla at col. 6, lines 37-39. The Head End of the cable network includes a cable modem termination system ("CMTS") and a provisioning server. Daruwalla FIG. 3.

Daruwalla describes that the provisioning server "may be configured as Dynamic Host Configuration Protocol ("DHCP") server in order to provide requesting cable modems (or devices which sit behind the cable modems) with IP addresses from outside the address space of the CMTS interface." Daruwalla at col. 6, lines 58-64. Before passing the IP address to the requesting cable modems, CMTS notes the IP address, identifies any VPN associated with the IP address, and associates the VPN with the service ID of the cable modems. Daruwalla at col. 11, lines 59-63 and FIG. 4. Apparently, this system enables the cable modems that are members of the same VPN to communicate in a manner that does not cause their respective packets to be routed outside the local network on which the cable modem resides. Daruwalla at col. 15, lines 59 to col. 16, line 1 and FIG. 10.

Daruwalla avails a cable modem of ability to communicate within the shared access network (e.g., HFC network) when communication involves another cable modem of the same

VPN; thus, alleviating the need to use the assigned IP address for routing packets outside the shared access network. To the extent that the second modem is not deemed to be on the same VPN, however, the IP addresses assigned to the cable modems are used to facilitate communications therebetween. In either case, Daruwalla discloses assigning IP addresses by the Head End. However, in neither case does Daruwalla describe doing so over a single communication tunnel. As such, Daruwalla fails to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1.

The Office Action appears to equate the provisioning server or CMTS to the host system recited in claim 1. Office Action at page 17, lines 9-13. Claim 1 has been amended to clearly recite that "the host system is located at one end of the single communication tunnel." In contrast, the provisioning server or CMTS described in Daruwalla is not located at the end of the tunnel. The tunnel described in Daruwalla and referred to by the Office Action extends from the cable modems and ends at the VPN gateway, across the HFC network and the backbone network. Daruwalla at col. 2, line 65 – col. 3, line 3. As such, Daruwalla fails to describe or suggest "the host system is located at one end of the single communication tunnel" and certainly does not describe or suggest "the host system... is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1.

Moreover, the Office Action suggests that "it would have been obvious to one of ordinary skill in the art at the time the invention was made to provide a tunnel from a cable modem under VPN to the Head End to establish a secure communication path between the cable modem and an authorized VPN gateway." Office Action at page 18, lines 2-5. Applicants respectfully disagree. Indeed, Applicants respectfully assert that Daruwalla teaches away from such a combination because such a combination would require each cable modem wishing to establish a tunnel be configured to support IPSec protocol, which Daruwalla describes as one of the disadvantages of the conventional VPN flow management. Daruwalla at col. 3, lines 9-10.

Instead, referring to FIG. 4 of Daruwalla, Daruwalla teaches a technique in which no tunnel is established between the cable modems and the Head End when assigning the IP address to the cable modems. And because it is the VPN gateway that provisions the VPN flow management in Daruwalla any communication tunnel would extend between the Head End and the VPN gateway and not between Head End and the cable modems. Daruwalla at col. 8, lines 51-56 (stating "one advantage of this approach is that VPNs can be provisioned at the CMTS or Head End... and there is no need for special software and/or hardware at the modem for managing VPN flows."). As such, Applicants respectfully assert that Daruwalla teaches way from configuring the cable modems to establish a tunnel between the cable modems and the Head End.

Accordingly, Daruwalla fails to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1 and similarly recited in independent claims 21 and 34. For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 1, 21, and 34 along with their dependent claims.

B. NTS in view of Ramp rejection

Claims 1, 21, and 34 are alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over NTS in view Ramp. Applicants respectfully assert that NTS and Ramp, either alone or in combination, fail to describe or suggest at least "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1 and similarly recited in claims 21 and 34.

NTS relates to enabling a single device at a remote location to access a company's network by building tunnel through the internet to the server that is attached to the company's network. NTS, chapter 1 at page 3, lines 1-2 and FIG. 2. As such, NTS merely describes establishing "a secure connection to private LAN over standard, non secure connection to the

internet." NTS, chapter 1 at page 1, lines 8-10. NTS further describes that once the tunnel is established the single device will be "assigned a new and different IP address, gateway and DNS server address." NTS, chapter 3 at page 3, lines 6-7. However, NTS fails to describe "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1.

Ramp does not remedy the shortcomings of the NTS to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1. Instead, Ramp relates to providing "an easy-to-use solution for providing shared internet access and VPN functionality." Ramp at page 1, lines 43-44. More particularly, Ramp describes "an integrated four-port Ethernet hub and connections for analog or ISDN modems." Ramp at page 1, lines 28-30. The Ethernet hub includes an external modem connection and apparently allows "multiple user sessions on a single tunnel." Ramp at page 1, lines 36-37. Ramp, however, is entirely silent as to the assignment of IP addresses.

The Office Action asserts that "it would have been obvious to one of ordinary skill in the art at the time of the invention to substitute the remote computer of NTS with a router, allowing multiple clients to use the same tunnel for VPN into the DHCP server of the NTS for benefit of sharing the same secure communication path from the home cable modem or DSL of NTS to DHCP server." Office Action at page 19, line 22 to page 20 line 1. Assuming *arguendo* this assertion is correct, it still fails to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1.

In particular, the assignment by a host system of a different independent Internet address to each of multiple different client devices over a single tunnel is not described or suggested by either NTS or Ramp. And combining the two by replacing NTS's remote computer with a

router, as suggested by the Examiner, to provide "the benefit of sharing the same secure communication path" does not result in such an assignment.

For example, Applicants respectfully assert that if NTS's remote computer were replaced by a router as suggested by the Examiner, the router may be a conventional NAT router that has been assigned a single Internet address for multiple devices sitting behind the conventional NAT router. The conventional NAT router enables the multiple devices sitting behind it to communicate over the same secure communication path over the internet without each of the devices being assigned a routable Internet address, much less being assigned the Internet addresses by a host system over a tunnel. Thus, the host system only recognizes the NAT router and not the devices communicating through the NAT router with the host system.

The distinction is an important one because the host system as recited in claim 1 is configured to assign an independent Internet address to each of the multiple home-networked client devices over the single communication tunnel. This enables the host system to recognize which of the multiple home-networked client devices communicate with the host over the single communication tunnel, thus empowering the host system to communicate individual information maintained by the host system to the multiple home-networked client devices (e.g., parental controls).

For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 1, 21, and 34 along with their dependent claims.

C. Reed and Kikinis in view Daruwalla rejection.

Claims 1, 21, and 34 are alternatively rejected under 35 U.S.C. 103(a) as being unpatentable over Reed in view of Kikinis and in further view of Daruwalla.

Applicants respectfully request reconsideration and withdrawal of the rejection because Reed, Kikinis, and Daruwalla, either alone or in combination, fail to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices

over the single communication tunnel," as recited in claim 1 and similarly recited in claims 21 and 34.

The Office Action concedes that "neither Reed nor Kikinis state a host system that assigns independent addresses to the home networked client devices." Office Action, page 21, lines 17-18. However, the Office Action asserts that Daruwalla teaches this feature. Applicants have illustrated above that Daruwalla clearly fails to describe or suggest "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1.

Accordingly, Applicants respectfully assert that Reed, Kikinis, and Daruwalla, either alone or in combination, fail to describe or suggest, "the host system is located at one end of the single communication tunnel and is configured to... assign independent Internet addresses to each of the multiple home-networked client devices over the single communication tunnel," as recited in claim 1 and similarly recited in claims 21 and 34.

For at least these reasons, Applicants respectfully request reconsideration and withdrawal of the rejection of claims 1, 21, and 34 along with their dependent claims.

Conclusion

It is believed that all of the pending issues have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this reply should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this reply, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

Please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: 4/17/06

KSL Kevin Greene 46,031
for W. Karl Renner
Reg. No. 41,265

Fish & Richardson P.C.
1425 K Street, N.W.
11th Floor
Washington, DC 20005-3500
Telephone: (202) 783-5070
Facsimile: (202) 783-2331

40338812.doc